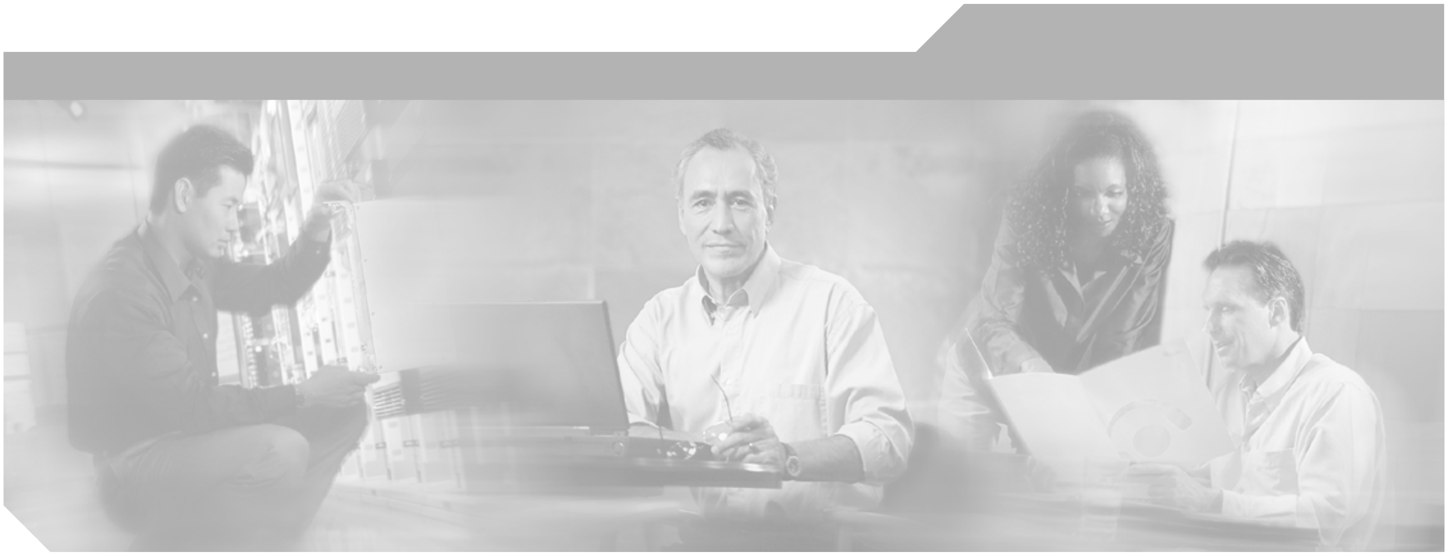


Cisco Catalyst Blade Switch 3040 for FSC Hardware Installation Guide

September 2006

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-10694-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco’s installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco’s written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.

- Move the equipment to one side or the other of the television or radio.

- Move the equipment farther away from the television or radio.

- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Catalyst Blade Switch 3040 for FSC Hardware Installation Guide

CONTENTS

Preface

Audience

This guide is for the networking or computer technician responsible for installing the Cisco Catalyst Blade Switch 3040 for FSC, referred to as the *blade switch,* in the Fujitsu Siemens Computers (FSC) PRIMERGY BX600 S2 blade server, referred to as the *BX600 system.* We assume that you are familiar with the concepts and terminology of Ethernet and local area networking.

Purpose

This guide describes the hardware features of the Cisco Catalyst Blade Switch 3040 for FSC. It describes the physical and performance characteristics of the blade switch, explains how to install it in the server chassis, and provides troubleshooting information.

This guide does not describe system messages that you might receive or how to configure your blade switch. For more information, refer to the blade switch software configuration guide, the blade switch command reference, and the blade switch system message guide on the Cisco.com Product Documentation home page.

Organization

This guide is organized into these chapters:

Chapter 1, “Product Overview,” is a physical and functional overview of the blade switch. It describes the blade switch ports, the standards they support, and the blade switch LEDs.

Chapter 2, “Blade Switch Installation,” contains the procedures on how to install the blade switch in the server chassis and how to make port connections.

Chapter 3, “Troubleshooting,” describes how to identify and resolve some of the problems that might arise when installing the blade switch.

Appendix A, “Technical Specifications,” lists the physical and environmental specifications for the blade switch and the regulatory agency approvals.

Appendix B, “Connector and Cable Specifications,” describes the connectors, cables, and adapters that can be used to connect to the blade switch.

Appendix C, “Configuring the Switch with the CLI-Based Setup Program,” has an installation and setup procedure for a standalone blade switch.

Conventions

This document uses these conventions and symbols for notes, cautions, and warnings:

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning **IMPORTANT SAFETY INSTRUCTIONS**
This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.
SAVE THESE INSTRUCTIONS (Statement 1071)

The safety warnings for this product are translated into several languages in the *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3040 for FSC* that ships with the product. The EMC regulatory statements are also included in that guide.

Related Publications

You can order printed copies of documents with a DOC-xxxxxx= number. For more information, see the "Obtaining Documentation" section on page ix.

These documents provide complete information about the blade switch and are available from this Cisco.com site:

http://www.cisco.com/en/US/products/ps6748/tsd_products_support_series_home.html

- *Cisco Catalyst Blade Switch 3040 for FSC Getting Started Guide* (order number DOC-7817759=)
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3040 for FSC* (order number DOC-7817760=)
- *Release Notes for the Cisco Catalyst Blade Switch 3040 for FSC, Cisco IOS Release 12.2(25)SEF* (not orderable but available on Cisco.com)

Note Before installing, configuring, or upgrading the blade switch, see the release notes on Cisco.com for the latest information.

- *Cisco Catalyst Blade Switch 3040 for FSC Software Configuration Guide* (not orderable but available on Cisco.com)
- *Cisco Catalyst Blade Switch 3040 for FSC Command Reference* (not orderable but available on Cisco.com)
- *Cisco Catalyst Blade Switch 3040 for FSC System Message Guide* (not orderable but available on Cisco.com)

- These compatibility matrix documents are available from this Cisco.com site:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

  - *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix* (not orderable but available on Cisco.com)
  - *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix* (not orderable but available on Cisco.com)
  - *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules* (not orderable but available on Cisco.com)

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created monthly and is released in the middle of the month. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation**.radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the magazine for Cisco networking professionals. Each quarter, *Packet* delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can subscribe to *Packet* magazine at this URL:

  http://www.cisco.com/packet

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

Product Overview

This chapter provides a functional overview of the Cisco Catalyst Blade Switch 3040 for FSC, referred to as the *blade switch*. The blade switch is installed in the Fujitsu Siemens Computers (FSC) PRIMERGY BX600 S2 blade server, referred to as the *BX600 system*.

You can connect the uplink ports to other devices such as switches, routers, Cisco Wireless Access Point workstations, Cisco IP phones, or other networking equipment. You can also connect standalone servers or PCs to those ports.

These topics are included:

- Features, page 1-1
- Front Panel Description, page 1-2
- Rear Panel Description, page 1-5
- Management Options, page 1-5

Features

The 16-port Gigabit Ethernet blade switch aggregates 10 internal servers and connects them to the network through 6 uplink ports. Refer to the blade switch software configuration guide for examples that show how you might deploy the blade switch in your network.

These are the blade switch features:

- 10 internal Gigabit Ethernet 1000BASE-X ports
- 1 console port
- 2 external 10/100/1000BASE-T copper Gigabit Ethernet ports
- 4 external small-form factor pluggable (SFP) module uplink ports that support 1000BASE-SX fiber optic and 10/100/1000BASE-T copper (only Cisco SFP modules are supported)

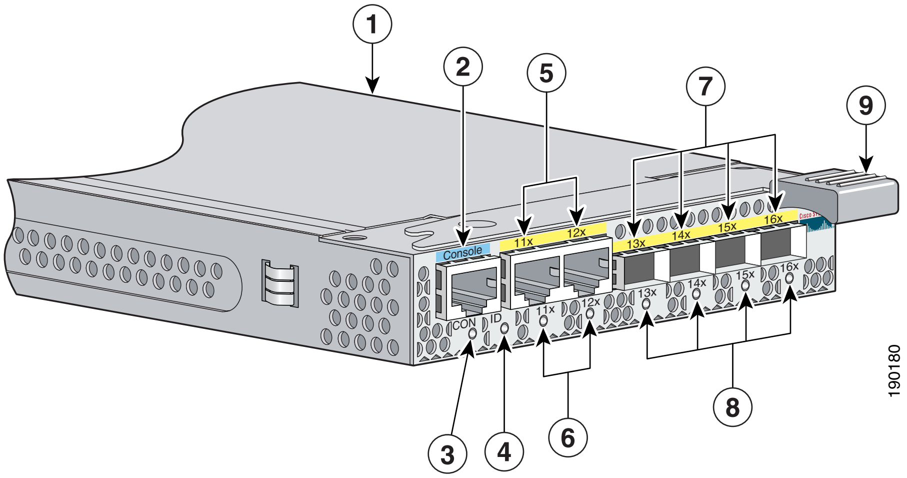
Note When installed in the blade switch, 1000BASE-T SFP modules operates at 10, 100, or 1000 Mbps in full-duplex mode or at 10 or 100 Mbps in half-duplex mode.

The BX600 system controls its own cooling and temperature. Its temperature sensor monitors the temperature of any blades that are installed. The BX600 system management blade controls the fan speed. The blade switch does not have its own fan.

Front Panel Description

Ten of the ports on the 16-port Gigabit Ethernet blade switch are internal 1000BASE-X ports that connect to the BX600 system through the backplane. Figure 1-1 shows the console port, the two external 10/100/1000BASE-T copper ports, and the four external SFP module uplink ports that support 1000BASE-SX and 10/100/1000BASE-T copper. Only Cisco SFP modules are supported.

Figure 1-1 The Cisco Catalyst Blade Switch 3040 for FSC



1	Blade switch	**6**	Gigabit Ethernet port LEDs
2	Console port	**7**	SFP module ports
3	Console port LED	**8**	SFP module port LEDs
4	System Status/ID LED	**9**	Release latch
5	External Gigabit Ethernet ports		

Each port has an associated LED. The BX600 system blade management board controls the System Status/ID LED.

Blade Switch Console Port

You can connect the switch module through its console port to a PC by using the RJ-45-to-DB9 female cable that ships with the product. If you need a spare cable, you can order a kit (part number ACS-DSBUASYN=) directly from Cisco. If you want to attach the switch module to any other device, such as a terminal server, you might need a different cable. For console port and adapter pinout information, see the "Connector and Cable Specifications" section on page B-1.

For information on the BX600 system management blade console port, see the BX600 system documentation.

10/100/1000 Ports

The two copper Ethernet ports operate at 10, 100, or 1000 Mbps and support autonegotiation and full-duplex operation. When set for autonegotiation, the port senses the speed and duplex settings of the attached device and advertises its own capabilities. If the connected device also supports autonegotiation, the blade switch port negotiates the best connection (that is, the fastest line speed that both devices support and full-duplex transmission if the attached device supports it) and configures itself accordingly. In all cases, the attached device must be within 328 feet (100 meters).

You can disable autonegotiation for the two 10/100/1000BASE-T ports by using the Cisco IOS command-line interface (CLI). For more information, see the blade switch command reference and software configuration guide.

The ten internal downlink ports are 1000BASE-X with no negotiation for speed or duplex.

Note 1000BASE-T traffic requires at least a Category 5 cable. 10BASE-T traffic can use Category 3 or Category 4 cables.

When you connect the blade switch to workstations, servers, routers, and Cisco IP Phones, be sure to use a straight-through Ethernet cable. When you connect the blade switch to another blade switch, use a crossover Ethernet cable. For any other type of connection, you can use a straight-through Ethernet cable. When you use a straight-through or crossover cable for 1000BASE-T connections, be sure to use a twisted four-pair, Category 5 cable for proper operation. Pinouts for the cables are described in Appendix B, “Connector and Cable Specifications.”

Note You can use the **mdix auto** interface configuration command in the CLI to enable the automatic medium-dependent interface crossover (auto-MDIX) feature. When the auto-MDIX feature is enabled, the blade switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a copper 10/100/1000 or 1000BASE-T SFP module port on the blade switch, regardless of the type of device on the other end of the connection.

The auto-MDIX feature is enabled by default. For configuration information for this feature, refer to the blade switch software configuration guide or command reference.

SFP Module Slots

The blade switch uses Gigabit Ethernet SFP modules to establish fiber-optic connections. These transceiver modules are field-replaceable, providing the uplink interfaces when inserted in an SFP module slot. You can use the SFP modules for Gigabit uplink connections to other switches. You use fiber-optic cables with LC or MT-RJ connectors to connect to a fiber-optic SFP module. You use a Category 5 cable with RJ-45 connectors to connect to a copper SFP module.

The four external SFP module ports operate at 1000 Mbps when fiber-optic SFP modules are installed and operate at 10/100/1000 Mbps when copper SFP modules are installed. Autonegotation is supported on copper SPF modules, but not on fiber-optic SFP modules.

See the blade switch release notes for the latest information about which SFP module types are supported.

For more information about the SFP modules, refer to your SFP module documentation.

LEDs

The blade switch has eight LEDs including an LED for each external port, one LED for the console port, and one LED used by BX600 system management board (see Figure 1-1). You can use the blade switch LEDs to monitor blade switch activity and performance. Graphical representations of the LEDs described in this section are visible in the device manager.

For more information about the BX600 management blade LEDS, see Table 2-1 on page 2-5.

System Status/ID LED

The System Status/ID LED is controlled by the BX600 system management blade and is used to identify a specific blade switch or other component in a rack from the management blade console. You can use the BX600 system web interface to identify a component, which triggers the specified device to light its ID LED.

Console Port LEDs

The blade switch console port LED is either green or amber. Table 1-2 describes the console port LED colors and their meanings.

Table 1-1 Meaning of Console Port LED Colors

LED Color	Meaning
Off	The bootloader is initializing.
Solid green	The blade switch console port is active.
Solid amber	The blade switch console port is inactive; the backplane console is active.
Solid green or amber	Cisco IOS is operating normally.

Port LEDs

The port LEDs display information about each individual port. The port LEDs are green, amber, or both. Table 1-2 describes the port LED colors and their meanings.

Table 1-2 Meaning of Port LED Colors

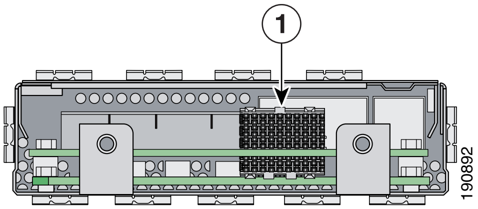
LED Color	Meaning
Off	No link established.
Solid green	Link established but no activity.
Blinking green	Traffic on an established link.
Solid amber	Port disabled, either error or STP[1] disabled.
Alternating green and amber	Link fault.

[1] STP = Spanning Tree Protocol

Rear Panel Description

The blade switch connects to the BX600 system through the backplane connector on the blade switch rear panel. See Figure 1-2.

Figure 1-2 Blade Switch Rear Panel



1	Backplane connector

Note You must engage the release latch to secure the connection to the backplane. See Figure 1-1.

Power Connectors

The BX600 system controls power to the blade switch. After the BX600 system detects the presence of the blade switch, it moves the blade switch to the full power state. The blade switch software is not involved in power control functions.

Management Options

This section describes management options for the blade switch:

- Using the Device Manager, page 1-5
- Using the Management Blade Web Interface, page 1-6
- Using the Command-Line Interface, page 1-8
- Other Management Options, page 1-8

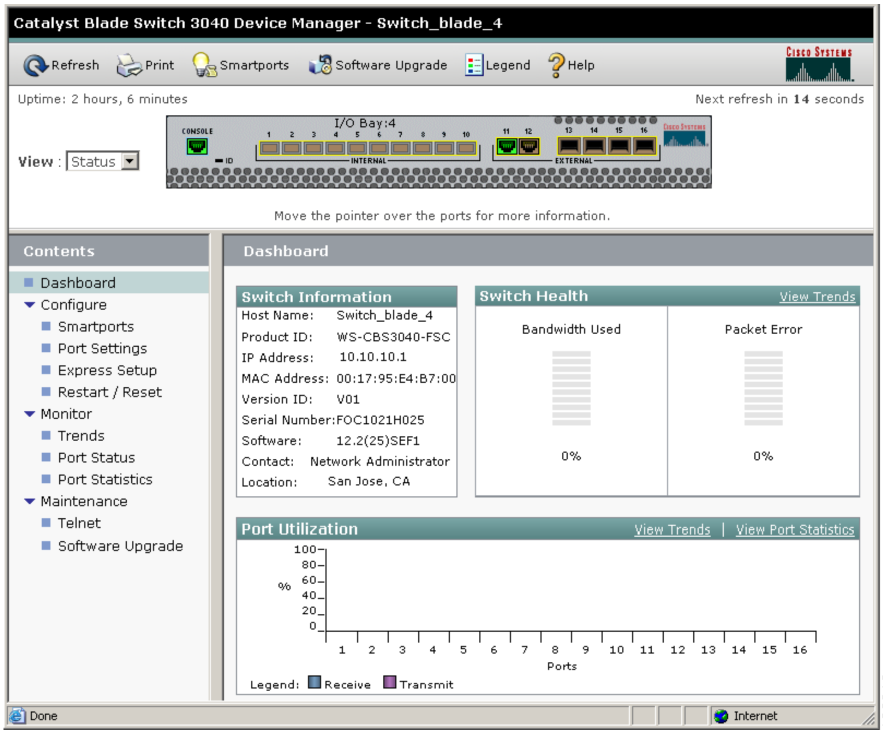
Using the Device Manager

The simplest way to manage the blade switch is by using the device manager that is in its memory. This is a web interface that offers quick configuration and monitoring. You can access the device manager from anywhere in your network through a web browser.

Follow these steps:

Step 1 Launch a web browser on your PC or workstation.

Step 2 Enter the blade switch IP address in the web browser, and press **Enter**. The device manager page appears.



Uptime: 2 hours, 6 minutes

Next refresh in **14** seconds

Move the pointer over the ports for more information.

Dashboard

Switch Information

Host Name: Switch_blade_4
Product ID: WS-CBS3040-FSC
IP Address: 10.10.10.1
MAC Address: 00:17:95:E4:B7:00
Version ID: V01
Serial Number: FOC1021H025
Software: 12.2(25)SEF1
Contact: Network Administrator
Location: San Jose, CA

Switch Health

Bandwidth Used	Packet Error
0%	0%

Port Utilization

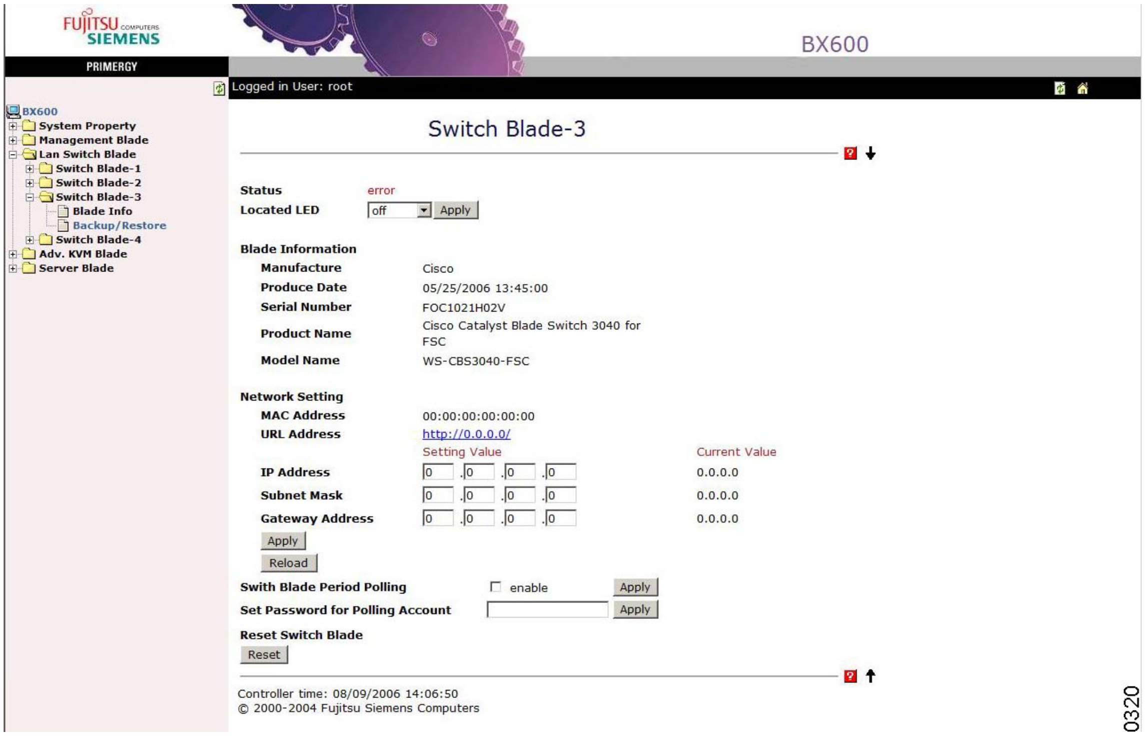
190216

Step 3 Use the device manager to perform basic blade switch configuration and monitoring. Refer to the device manager online help for more information.

Using the Management Blade Web Interface

You can monitor and manage the blade switches through the BX600 system web interface. Follow these steps:

1. Launch a web browser on your PC or workstation.
2. Enter the BX600 system IP address in the web browser, and press **Enter**. The web interface appears.
3. Click **Switch Blade 1**, **Switch Blade 2**, and so on to see the information for a specific blade switch.



Switch Blade-3

Status error
Located LED off

Blade Information
Manufacture Cisco
Produce Date 05/25/2006 13:45:00
Serial Number FOC1021H02V
Product Name Cisco Catalyst Blade Switch 3040 for FSC
Model Name WS-CBS3040-FSC

Network Setting
MAC Address 00:00:00:00:00:00
URL Address http://0.0.0.0/

	Setting Value	Current Value
IP Address	0 .0 .0 .0	0.0.0.0
Subnet Mask	0 .0 .0 .0	0.0.0.0
Gateway Address	0 .0 .0 .0	0.0.0.0

Swith Blade Period Polling □ enable
Set Password for Polling Account
Reset Switch Blade

Controller time: 08/09/2006 14:06:50
© 2000-2004 Fujitsu Siemens Computers

You can do these tasks:

- In the Located LED field, choose **on** or **off**, and click **Apply** to locate the blade switch.
- Under Network Setting, click the URL Address field to open the blade switch web interface.
- To reset the IP address, the subnet mask, or the gateway address, enter the new settings in the appropriate field, and click **Apply** and **Reload**. These settings apply only to VLAN 1. If you are using a management VLAN other than VLAN 1, the applied settings might not produce the intended results. See the BX600 system documentation for more information about setting these fields.
- To enable polling, click **Enable** and **Apply**. The default polling period is 300 seconds. To begin polling immediately, after you click **Enable** and **Apply**, click **Reset** under Reset the Switch Blade. Before you manage the blade switch from its console port, we recommend that you disable polling.
- If you configured a password for the blade switch through the management blade console menu, you must enter that password in the Set Password for Polling Account field, and click **Enable**. Otherwise, leave this field blank.
- Click **Reset** to reset the blade switch.

For more information about using this interface, see the *PRIMERGY BX Blade Server Systems RemoteView Management Blade User Interface Description*.

Using the Command-Line Interface

You can enter Cisco IOS commands and parameters through the CLI. Access the CLI either by connecting your PC directly to the blade switch console port or through a Telnet session from a remote PC or workstation.

Follow these steps:

Step 1 Connect the supplied console cable to the standard 9-pin serial port on the PC. Connect the other end of the cable to the console port on the blade switch.

Step 2 Start a terminal-emulation program on the PC.

Step 3 Configure the PC terminal emulation software for:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit
- No flow control

Step 4 Use the CLI to enter commands to configure the blade switch. See the blade switch software configuration guide and command reference for more information.

For quick setup instructions that use the CLI, go to Appendix C, “Configuring the Switch with the CLI-Based Setup Program.”

Other Management Options

You can use SNMP management applications such as CiscoWorks Small Network Management Solution (SNMS) to configure and manage the blade switch. You also can manage it from an SNMP-compatible workstation that is running platforms such as HP OpenView or SunNet Manager.

Network Configurations

Refer to the blade switch software configuration guide on Cisco.com for an explanation of network configuration concepts. The software configuration guide also provides examples of network configurations that use the blade switch to create dedicated network segments that are interconnected through Gigabit Ethernet connections.

CHAPTER 2

Blade Switch Installation

This chapter provides instructions on how to install your Cisco Catalyst Blade Switch 3040 for FSC, referred to as the *blade switch*, in the Fujitsu Siemens PRIMERGY BX600 S2 system, and to set up and configure it. The PRIMERGY BX600 S2 system, referred to as the *BX600 system*, supports up to four Ethernet blade switches, which are installed in its blade bays. The blade switch is installed in one of the I/O blade bays on the rear panel of the BX600 system.

This chapter also describes how to interpret the power-on self-test (POST) that ensures proper operation and how to make connections to the blade switch.

Read the topics and perform the procedures in this order:

- Preparing for Installation, page 2-1
- BX600 System Architecture, page 2-4
- Overview of Steps for Installing and Initially Configuring the Blade Switch, page 2-6
- Installing and Removing SFP Modules, page 2-15
- Connecting to the 10/100/1000 Ports, page 2-18
- Connecting to SFP Modules, page 2-19
- Where to Go Next, page 2-20

Preparing for Installation

This section covers these topics:

- Warnings, page 2-2
- Installation Guidelines, page 2-3
- Verifying Package Contents, page 2-3

Warnings

These warnings are translated into several languages in the *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3040 for FSC* that ships with the product. The EMC regulatory statements are also included in that guide.

Warning **To prevent the switch from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 113°F (45°C). To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings.** Statement 17B

Warning **Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.** Statement 43

Warning **Ethernet cables must be shielded when used in a central office environment.** Statement 171

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

Warning **Read the installation instructions before connecting the system to the power source.** Statement 1004

Warning **Class 1 laser product.** Statement 1008

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

Warning **For connections outside the building where the equipment is installed, the following ports must be connected through an approved network termination unit with integral circuit protection. 10/100/1000 Ethernet** Statement 1044

Warning **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

Installation Guidelines

Before you install the blade switch in the BX600 system, consider these points:

- Review and become familiar with the safety guidelines in the *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3040 for FSC* that accompanies this guide.
- Review and become familiar with the BX600 system safety guidelines in the BX600 system documentation.
- Review and become familiar with the temperature, power, and grounding requirements specified in the BX600 system documentation.

Caution To prevent electrostatic-discharge (ESD) damage when installing blade switches, follow your normal board and component handling procedures.

Note When you install a blade switch, you do not need to power down the BX600 system.

Note The initial configuration assumes that the blade switch was never configured, that it is in the same state as when it was received, and that it is not configured with a default username and password.

Be sure to observe these requirements:

- For copper Ethernet ports, cable lengths from the blade switch to connected devices can be up to 328 feet (100 meters).
- See the documentation for the SFP module for more information about cable specifications for the SFP module connections. Each port must match the wave-length specifications on the other end of the cable, and the cable must not exceed the stipulated cable length for reliable communications.

  Note When using shorter lengths of single-mode fiber-optic cable, you might need to insert an inline optical attenuator in the link to avoid overloading the receiver.

- Operating environment is within the ranges listed in Appendix A, “Technical Specifications.”
- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures. Make sure the cabling is safely away from other devices that might damage the cables.

Verifying Package Contents

Note Carefully remove the contents from the shipping container, and check each item for damage. If any item is missing or damaged, contact your Cisco representative or reseller for support. Return all packing material to the shipping container, and save it.

These items ship with your blade switch:

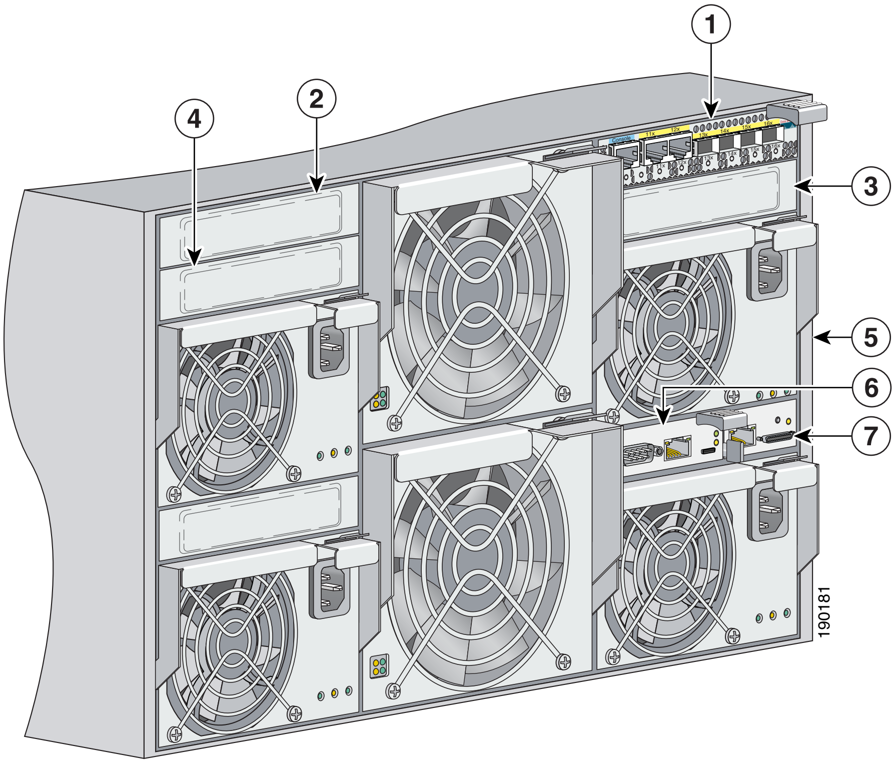
- Console cable
- *Cisco Catalyst Blade Switch 3040 for FSC Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3040 for FSC*
- Registration card

Note If the blade switches are ordered with the BX600 system, the blade switches are already installed, and no unpacking is required. The unpacking procedure applies only if a blade switch is ordered separately.

BX600 System Architecture

The four chassis I/O module slots are on the rear panel (see Figure 2-1). You can insert blade switches into the NET1, NET2, NET3, and NET4 I/O blade bays.

Figure 2-1 Rear View of the BX600 System

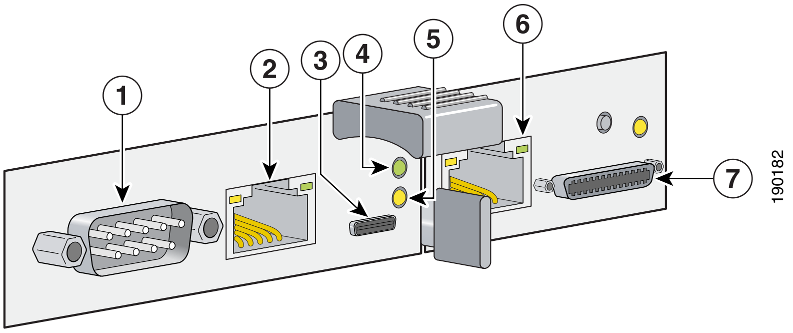


1	NET1 slot (with blade switch installed)	**5**	Rear panel of the BX600 system
2	NET2 slot	**6**	BX600 system management blade
3	NET3 slot	**7**	Advanced KVM[1] blade
4	NET4 slot		

[1] KVM = Keyboard, video, and mouse connection

Figure 2-2 shows the BX600 system management blade on the left and an optional advanced KVM blade on the right.

Figure 2-2 BX600 System Management and Advanced KVM Blades



1	RS-232 serial port	**5**	Failure indicator LED
2	Ethernet port	**6**	Advanced KVM blade Ethernet port
3	I2C connector[1]	**7**	KVM connector [2]
4	Green master indicator LED		

[1] A proprietary Intelligent Platform Management Interface (IPMI) connector for Fujitsu Siemens Computers service applications

[2] The KVM connector uses a special cable to connect a VGA monitor, a PS2 keyboard, and a PS2 mouse.

Table 2-1 describes the BX600 system management blade LEDs:

Table 2-1 Management Blade LED Descriptions

LED	Description
Ethernet port	Green: On shows link is up; blinking shows power is on. Amber: On shows LAN is active; blinking shows power is on.
Master (green)	On: The management blade is the master, responsible for managing the entire system. Off: The management blade is a slave—a standby or backup of the master management blade. Blinking: The management blade is in special mode.
Failure (amber)	On: If only one management blade is installed, it has failed. Off: This management blade is operating normally. Blinking: The management blade is running in power-on mode, that is, generating a heartbeat for the master/slave selection.

Note For more information about the master and failure management blade LEDs or the advanced KVM management blade, see the *PRIMERGY BX600 Basic Unit Operating Manual.*

Consider these requirements before you install your blade switch:

- The NET1 and NET2 slots are a pair. If the NET2 slot is used, the I/O blade in the NET2 slot must be the same type as the one in the NET1 slot.
- The NET3 and NET4 slots are a pair. If the NET4 slot is used, the I/O blade in the NET4 slot must be the same type as the one in the NET3 slot.
- If the blade switch is installed in the NET3 and NET4 slots, an Ethernet I/O module (daughter card) must be installed on the BX600 server.

For more information about the components of the BX600 system, see the *PRIMERGY BX600 Basic Unit Operating Manual*.

Overview of Steps for Installing and Initially Configuring the Blade Switch

You can install and configure the blade switch by using either of two methods. In each, you start a terminal-emulation program on a PC. The terminal-emulation software—a PC application such as Hyperterminal or ProcommPlus—makes communication between the blade switch and your PC or terminal possible. The PC communicates with the blade switch either through its console port or through the console port of BX600 system management blade.

- To set up the blade switch through its console port, start with the next section, "Installing the Blade Switch in the BX600 System."
- To set up the blade switch through the BX600 system management blade, first connect it to a PC to run the terminal emulation program and to interact with the console menu. Do this before you install the blade switch into the BX600 system. Start with the "Connecting through the BX600 System Management Blade" section on page 13.

Installing the Blade Switch in the BX600 System

Follow these steps to install the blade switch in the BX600 system:

Step 1 Obtain and make note of this information from your system administrator before you begin the blade switch installation:

- Switch IP address
- Subnet mask (IP netmask)
- Default gateway (router)
- Enable secret password (encrypted)
- Enable password (not encrypted)
- Telnet password
- SNMP community strings (optional)

Step 2 Touch the blade switch static-protective package to unpainted metal on the BX600 system for at least 2 seconds.

Step 3 Remove any dummy blade from the slot.

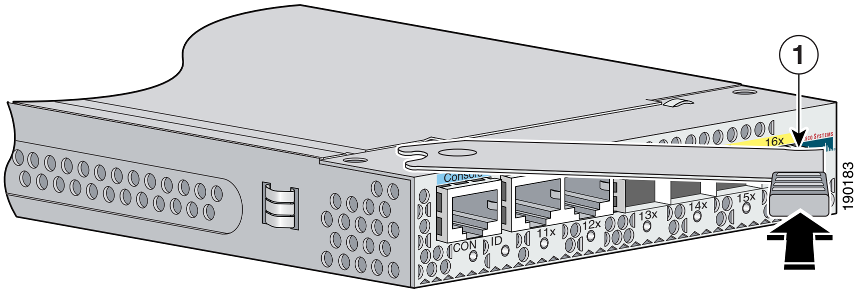
Caution Keep dummy blades for future use. If you remove the blade switch and do not replace it with another one, you must reinstall a dummy blade in that slot.

Step 4 Remove the blade switch from its static-protective package.

Step 5 Select the I/O slot in which to install the blade switch. Follow the installation requirements listed in the "BX600 System Architecture" section on page 2-4.

Step 6 Ensure that the release latch on the blade switch is in the open position. (See Figure 2-3.)

Figure 2-3 Open the Blade Switch Release Latch



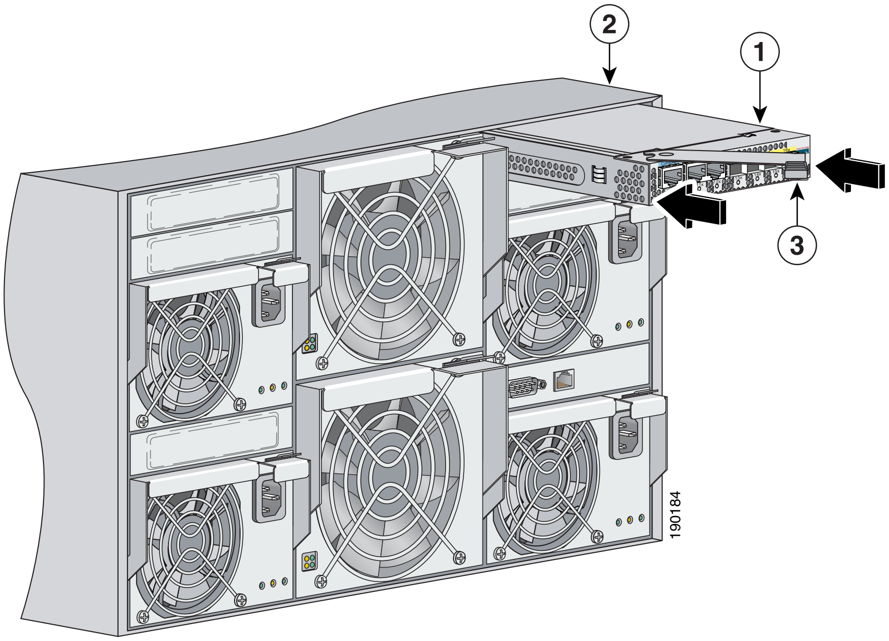
1	Release latch in open position

Step 7 Slide the blade switch into the slot until it stops.

Step 8 Push the release latch on the front of the blade switch toward the right and into the closed position.

Figure 2-4 shows the blade switch being inserted into the BX600 system.

Figure 2-4 Inserting the Blade Switch into the BX600 System



1	Blade switch	**3**	BX600 system
2	Release latch		

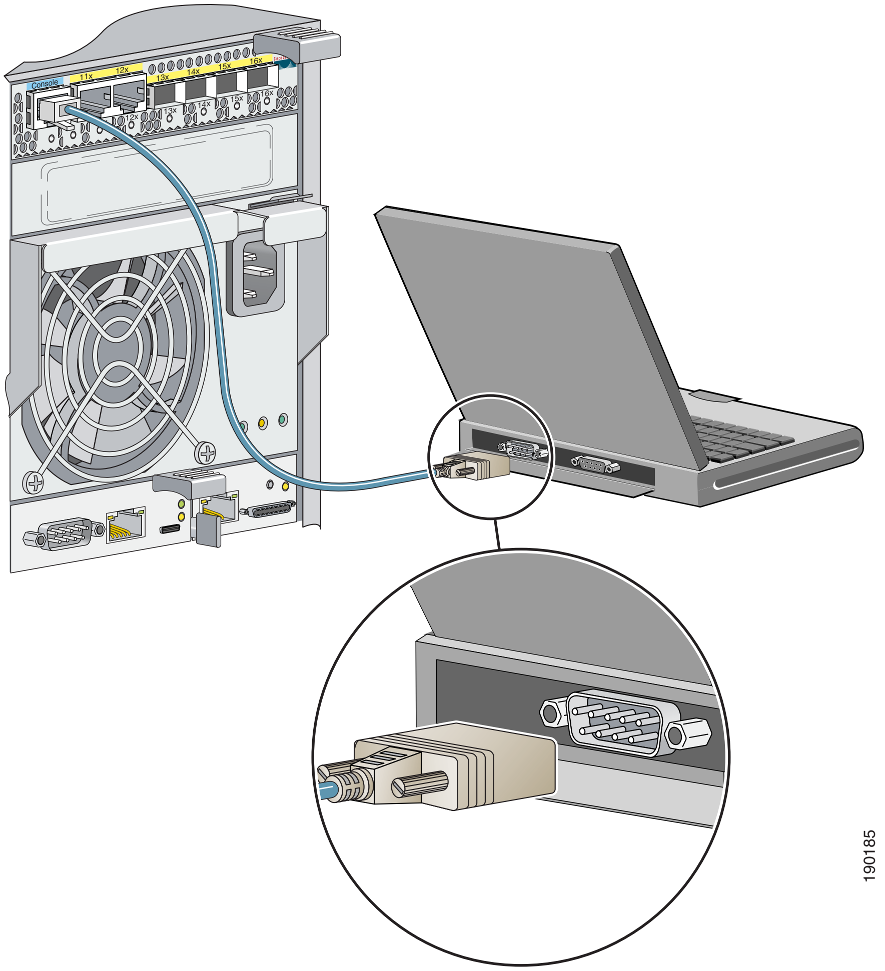
Step 9 If you are setting up the blade switch through the its console port, go to the "Connecting through the Blade Switch Console Port" section on page 2-8. If you are setting it up through the BX600 system management blade, go to Step 6 in the "Connecting through the BX600 System Management Blade" section on page 2-9.

Connecting through the Blade Switch Console Port

Follow these steps to set up the blade switch by connecting it to a PC through the blade switch console port:

Step 1 Connect one end of the console cable to the blade switch console port. Connect the other end of the cable to the serial port of a PC. (See Figure 2-5.)

Figure 2-5 Connecting through the Blade Switch Console Port



Step 2 Start the terminal emulation session so that you can see the output display from the POST.

Step 3 On the PC terminal emulation program:

a. Set the data format to 8 data bits, 1 stop bit, and no parity.

b. Set the terminal emulation speed to 9600 baud.

c. Set the flow control to None.

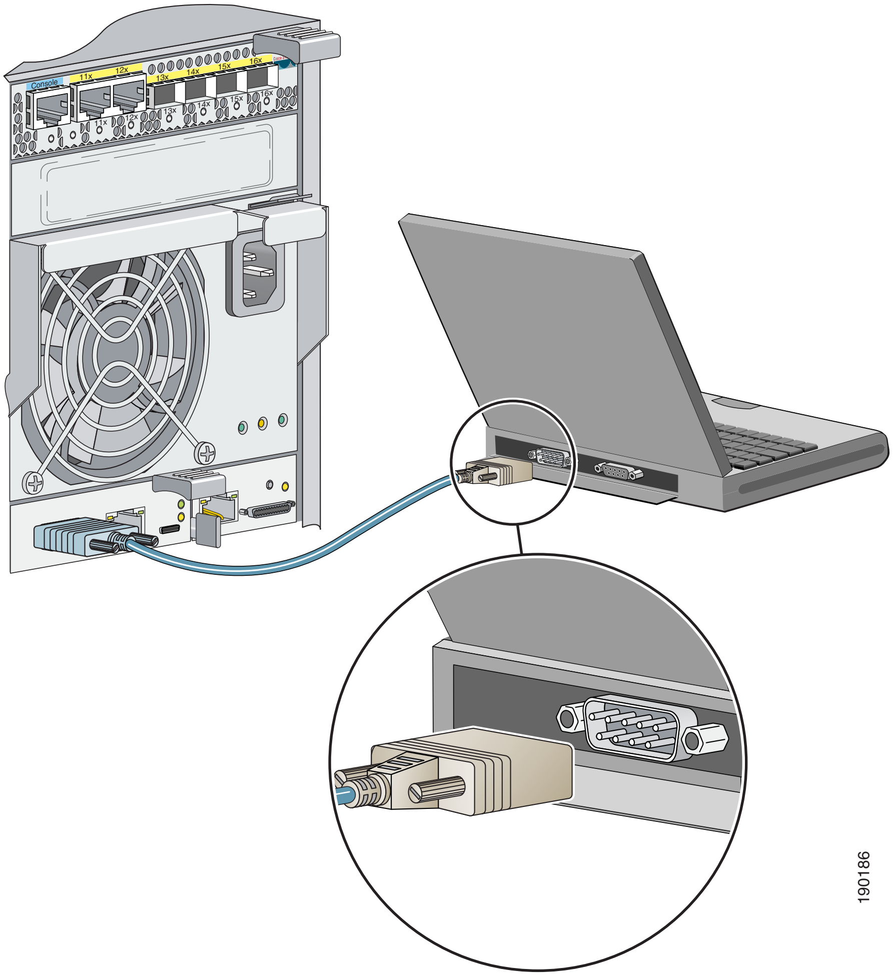
Step 4 Go to the "Waiting for POST to Complete" section on page 2-12 to finish configuring the blade switch.

Connecting through the BX600 System Management Blade

Follow these steps to set up the blade switch by connecting to a PC through the BX600 system management blade console port:

Step 1 Connect one end of a DB9 null-modem or a crossover cable to the RS-232 console serial port of the associated management blade. Connect the other end of the cable to the RS-232 console serial port of the PC. (See Figure 2-6.)

Figure 2-6 Connecting through the BX600 System Management Blade



Step 2 On the PC terminal emulation program:

a. Set the data format to 8 data bits, 1 stop bit, and no parity.

b. Set the terminal emulation speed to 115200 baud.

c. Set Flow Control to none.

d. Under Properties, select VT100 for Emulation mode.

e. Select Terminal keys for Function, Arrow, and Ctrl keys. Make sure that you select Terminal keys, not Windows keys.

Step 3 On the console monitor, the management blade application displays a login screen. Log in by using these defaults:
username **root**
password **root**

The management blade Console Main menu appears.

Note If the BX600 system is already configured, obtain the management blade username and password from the system administrator. If you use *root* for the username and password, you must change them later. See the BX600 system documentation for more information.

Step 4 To power on the BX600 system, use these menu choices in the Console Main menu:

a. Enter **1** (Management Agent). The Management Agent menu appears.

b. Enter **3** (System Information). The System Information menu appears.

c. Enter **2** (Power Supply). The Power Supply menu appears.

d. Enter **1** (Power Control). The Power Control menu appears.

e. Enter **2** to power on the BX600 system.

f. Enter **0** at each menu to return to the main menu.

Note The management blade console menu uses a hot key to return to a previous menu. The default is set to **Ctrl–Q**. For some terminal emulation programs, **Ctrl–Q** might not work. You can reset the hot key in the Console Redirection Table menu. Choose a character from A-Z, excluding M. The hot key to exit console redirection and return to the previous mode is then Ctrl + the character you have set. For more information, see the BX600 system documentation.

Step 5 Install the blade switch by following the instructions in the "Installing the Blade Switch in the BX600 System" section on page 2-6, and then return to this section.

Step 6 After you have installed the blade switch in the BX600 system, wait for the blade switch port 11x LED to blink green before you continue.

Step 7 Enter **3** (Console Redirection) on the main menu:

```
+----------------------------------------------------------------------------+
|                          Console Menu                    page_root
+----------------------------------------------------------------------------+
(1) Management Agent
(2) Emergency Management Port
(3) Console Redirection
(4) TFTP update
(5) Logout
(6) Reboot Management Blade
(7) System Information Dump
(8) Command Line Interface
Enter selection: 3
```

The Console Redirection Table menu appears.

Step 8 Enter **2** (Console Redirect Switch Blade) in the Console Redirection Table menu to redirect the console to the blade switch:

```
+----------------------------------------------------------------------------+
|        Console Redirection Table                         page_3
+----------------------------------------------------------------------------+
(1) Console Redirect Server Blade
(2) Console Redirect Switch Blade
(3) Set Return Hotkey , Ctrl+(a character) : Q Enter selection or type (0) to quit: 2
```

The Console Redirection Switch Blade menu appears.

Step 9 Enter **1** in the Console Redirect Blade Switch menu if you are configuring the blade switch in the NET1 slot, **2** if you are configuring the blade switch in the NET2 slot, and so on:

```
+------------------------------------------------------------------------------+
|        Console Redirect Switch Blade                     page_3_2
+------------------------------------------------------------------------------+
(1) Console Redirect Switch Blade_1
(2) Console Redirect Switch Blade_2
(4) Console Redirect Switch Blade_4
Enter selection or type (0) to quit: 1
```

Step 10 Go to "Waiting for POST to Complete" section on page 2-12 to finish configuring the blade switch.

Note If the blade switch is already installed and powered up when you use the BX600 system management blade console menu, you must reboot the switch to display the system configuration dialog. Enter **enable** at the user EXEC (`Switch>`) prompt, then enter **reload** at the privileged EXEC mode (`Switch#`) prompt.

Waiting for POST to Complete

Follow these steps:

Step 1 Wait several minutes for the blade switch to complete the POST.

The POST is complete when the System Status/ID LED is off and the Console LED is solid green or amber. If the blade switch fails POST because of a misconfiguration or error, the System Status/ID LED blinks green and the Console LED is off.

Note POST errors are usually fatal. Call Cisco Customer Support immediately if your blade switch fails POST.

Step 2 Wait for the blade switch to complete flash initialization. When you see the prompt `Press Return to Get Started!`, wait for any interface status information output to finish its appearance, then press **Return** or **Enter**.

Step 3 Make sure that the System Status/ID LED is off, and that the Console LED is green or amber. The blade switch is now operating properly.

Step 4 Continue with the "Completing the Initial Configuration" section on page 2-13 for instructions on setting up and initially configuring the blade switch.

Completing the Initial Configuration

Follow these steps to complete the setup program and to create an initial configuration.

Note For information about how to automatically configure the blade switch, see the "Assigning the Switch IP Address and Default Gateway" chapter in the blade switch configuration guide.

Step 1 After you have pressed **Enter** or **Return** after the prompt to start the system configuration dialog, enter **yes** at these prompts:

```
Would you like to terminate autoinstall? [yes]: yes
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
```

Step 2 Enter a hostname for the blade switch after the prompt, and press **Return**.

The hostname is limited to 20 characters. Do not use *-n*, where n is a number, as the last character in a host name for any blade switch.

Step 3 Enter an enable secret password, and press **Return**.

The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows spaces, but ignores leading spaces. The secret password is encrypted, and the enable password is in plain text.

Step 4 Enter an enable password, and press **Return**.

Step 5 Enter a virtual terminal (Telnet) password, and press **Return**.

The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

Step 6 (Optional) Configure Simple Network Management Protocol (SNMP) by responding to the prompts.

To configure SNMP later, press **Return** (which applies the default of no). If you accept the default, you can configure SNMP later through the CLI.

```
Configure SNMP Network Management? [no]:
```

To configure SNMP now, enter **yes**.

```
Configure SNMP Network Management? [no]: yes
Community string [public]: public
```

The Current interface summary displays.

Step 7 Enter **vlan1** for the interface name at this prompt:

```
Enter interface name used to connect to the management network from the above interface
summary.
```

Step 8 To configure the interface, enter **Yes** after the prompt, and then enter the blade switch IP address and subnet mask. Press **Return**.

The IP address and subnet mask shown here are examples:

```
Configuring interface Vlan1:
Configure IP on this interface? [yes]: Yes
IP address for this interface [10.0.0.1]: 10.0.0.1
Subnet mask for this interface [255.255.255.0] : 255.255.255.0
Class A network is 10.0.0.1, 21 subnet bits; mask is /21
```

Step 9 Enter **no** when the prompt asks you if you would like to enable the blade switch as a cluster command switch. This is a standalone blade switch.

```
Would you like to enable as a cluster command switch? [yes/no]: no
```

Note The Cisco Catalyst Blade Switch 3040 for FSC does not support clustering.

You have now completed the initial configuration. An example of the output is shown here:

```
The following configuration command script was created:
hostname switch1
enable secret 5 $1$cagJ$e4LP91PNazfdADoNAZm6y0
enable password enable_password
line vty 0 15
password terminal-password
snmp-server community public
!
!
interface Vlan1
no shutdown
ip address 10.0.0.1 255.255.255.0
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2

. . . (output truncated)


interface GigabitEthernet0/16
!
end
```

Step 10 These choices appear. Enter **2**, and then press **Return**.

```
[0] Go to the IOS command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

If you want to save the configuration and use it the next time the switch reboots, save it
in NVRAM by selecting option 2.

Enter your selection [2]:2

Make your selection, and press Return.
```

Step 11 If you plan to set up more than one blade switch, enter **Ctrl-Q** to return to the Console Redirect Switch Blade menu, and choose the next blade switch. When you have set up all of the blade switches, enter **0** on the Console Redirect Switch Blade menu to return to the management blade Console Main menu. This re-enables the blade switch console port.

Step 12 Disconnect the BX600 system serial port or the blade switch console port from the PC. See the "Management Options" section on page 1-5 for information about configuring and managing the blade switch.

If you need to rerun the system configuration dialog, see the "Resetting the Switch Configuration" section on page 2-15.

Resetting the Switch Configuration

This section describes how to reset the switch configuration by rerunning the initial configuration dialog (System Configuration Dialog). These are reasons why you might want to reset the switch:

- You installed the switch in your network and cannot connect to it because you assigned the wrong IP address.
- You want to clear all configuration from the switch and assign a new IP address.

⚠ **Caution** Resetting the switch deletes the configuration and reboots the switch.

To reset the switch, at the switch prompt, enter **enable** and press **Return or Enter**. At the Privileged EXEC prompt, `switch#`, enter **setup** and press **Return or Enter**.

The switch displays the prompt to run the initial configuration dialog. See the "Completing the Initial Configuration" section on page 2-13 to re-enter the configuration information and set up your switch.

Installing and Removing SFP Modules

These sections describe how to install and remove SFP modules. The modules are inserted into the SFP module slots on the blade switch. These field-replaceable modules provide uplink interfaces.

You can use any combination of SFP modules. Refer to the blade switch release notes for the list of the supported SFP modules. Each port must match the wave-length specifications on the other end of the cable, and the cable must not exceed the stipulated cable length for reliable communications. See the "Installation Guidelines" section on page 2-3 for cable stipulations for SFP connections.

Use only Cisco SFP modules. Each SFP module has an internal serial EEPROM that is encoded with security information. This encoding provides a way for Cisco to identify and validate that the SFP module meets the requirements for the blade switch. For detailed instructions on installing, removing, and cabling the SFP module, refer to your SFP module documentation.

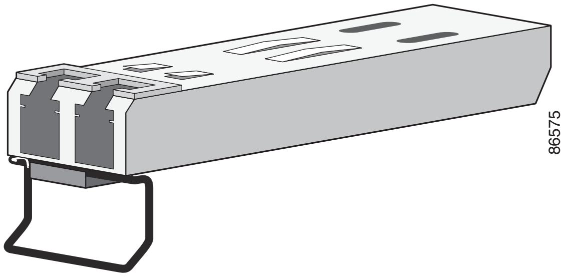
Installing SFP Modules into SFP Module Slots

Figure 2-7 shows an SFP module that has a bale-clasp latch.

⚠ **Caution** We strongly recommend that you do not install or remove fiber-optic SFP modules with cables attached because of the potential damage to the cables, the cable connector, or the optical interfaces in the SFP module. Disconnect all cables before removing or installing an SFP module.

Removing and installing an SFP module can shorten its useful life. Do not remove and insert SFP modules more often than is absolutely necessary.

Figure 2-7 SFP Module with a Bale-Clasp Latch



To insert an SFP module into the module slot, follow these steps:

Step 1 Attach an ESD-preventive wrist strap to your wrist and to a bare metal surface on the chassis.

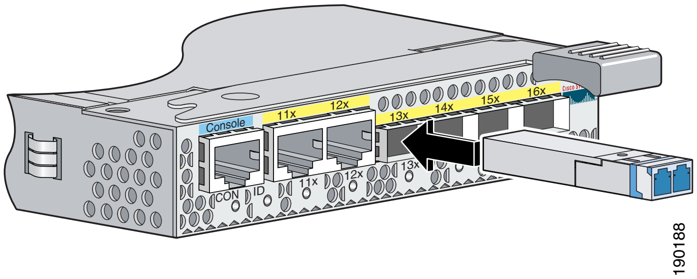
Step 2 Find the send (TX) and receive (RX) markings that identify the top side of the SFP module.

Note On some SFP modules, the send and receive (TX and RX) markings might be replaced by arrows that show the direction of the connection, either send or receive (TX or RX).

Step 3 Align the SFP module in front of the slot opening.

Step 4 Insert the SFP module into the slot until you feel the connector on the module snap into place in the rear of the slot. (See Figure 2-8.)

Figure 2-8 Installing an SFP Module into an SFP Module Slot



Removing SFP Modules from SFP Module Slots

To remove an SFP module from a module receptacle, follow these steps:

Step 1 Attach an ESD-preventive wrist strap to your wrist and to a bare metal surface on the chassis.

Step 2 Disconnect the cable from the SFP module.

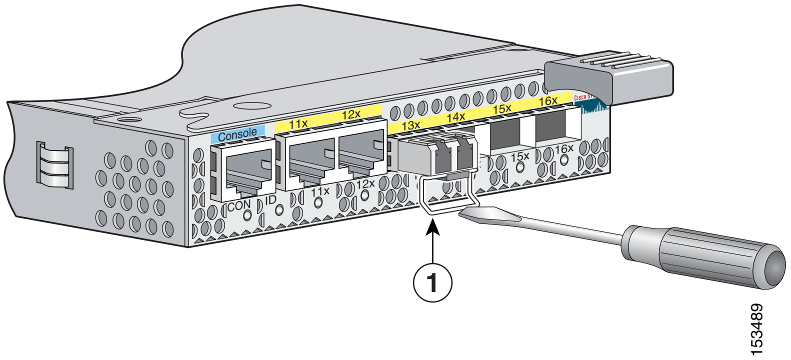
Tip For reattachment, note which cable connector plug is send (TX) and which is receive (RX).

Step 3 For fiber-optic SFP modules, insert a dust plug into the optical ports of the SFP module to keep the optical interfaces clean.

Step 4 Unlock and remove the SFP module, as shown in Figure 2-9.

If the module has a bale-clasp latch, pull the bale out and down to eject the module. If the bale-clasp latch is obstructed and you cannot use your index finger to open it, use a small, flat-blade screwdriver or other long, narrow instrument to open the bale-clasp latch.

Figure 2-9 Removing a Bale-Clasp Latch SFP Module by Using a Flat-Blade Screwdriver



1	Bale clasp

Step 5 Grasp the SFP module between your thumb and index finger, and carefully remove it from the module slot.

Step 6 Place the removed SFP module in an antistatic bag or other protective environment.

Connecting to the 10/100/1000 Ports

The 10/100/1000 ports configure themselves to operate at the speed of attached devices. If the attached ports do not support autonegotiation, you can explicitly set the speed and duplex parameters. Connecting devices that do not autonegotiate or that have their speed and duplex parameters manually set can reduce performance or result in no linkage.

To maximize performance, choose one of these methods for configuring the Ethernet ports:

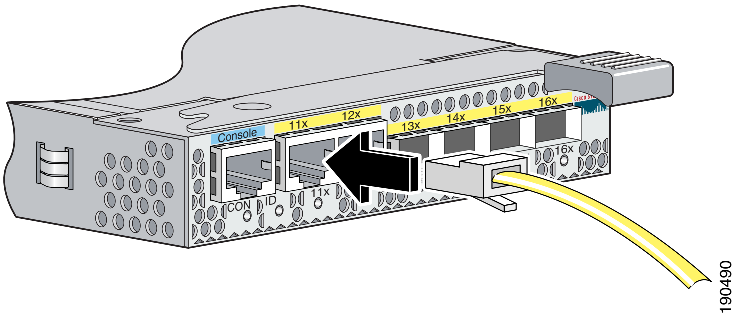
- Let the ports autonegotiate both speed and duplex.
- Set the port speed and duplex parameters on both ends of the connection.

Follow these steps to connect to 10BASE-T, 100BASE-TX or 1000BASE-T devices:

Caution To prevent electrostatic-discharge (ESD) damage, follow your normal board and component handling procedures.

Step 1 When connecting to workstations, servers, routers, and Cisco IP Phones, connect a straight-through cable to an RJ-45 connector on the front panel. (See Figure 2-10.) When connecting to switches or repeaters, use a crossover cable. (See the "Cable and Adapter Specifications" section on page B-3 for cable-pinout descriptions.)

Figure 2-10 Connecting to an Ethernet Port



Note When you connect to 1000BASE-T-compatible devices, be sure to use a twisted four-pair, Category 5 cable.

Step 2 Connect the other end of the cable to an RJ-45 connector on the other device. The port LED turns on when both the blade switch and the connected device have established link.

The port LED is amber while Spanning Tree Protocol (STP) discovers the topology and searches for loops. This takes about 30 seconds, and then the port LED turns green. If the port LED does not turn on, the device at the other end might not be turned on, or there might be a cable problem or a problem with the adapter installed in the attached device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

You can use the **mdix auto** interface configuration command in the CLI to enable the automatic medium-dependent interface crossover (auto-MDIX) feature. When the auto-MDIX feature is enabled, the blade switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a copper 10/100/1000 module port on the blade switch, regardless of the type of device on the other end of the connection.

The auto-MDIX feature is enabled by default.

Step 3 Reconfigure and reboot the connected device if necessary.

Step 4 Repeat Steps 1 through 3 to connect each device.

Connecting to SFP Modules

This section describes how to connect to SFP modules. For instructions on how to connect to fiber-optic SFP modules, see the "Connecting to Fiber-Optic SFP Modules" section.

For instructions about how to install or remove an SFP module, see the "Installing and Removing SFP Modules" section on page 2-15.

Connecting to Fiber-Optic SFP Modules

Follow these steps to connect a fiber-optic cable to an SFP module:

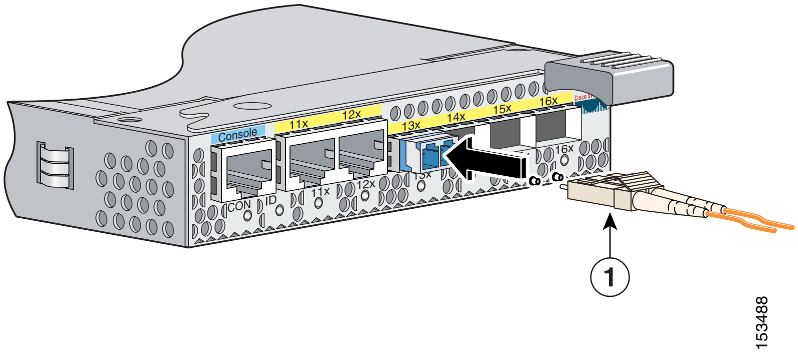
⚠ **Caution** Do not remove the rubber plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the SFP module ports and cables from contamination and ambient light.

Before connecting to the SFP module, be sure that you understand the port and cabling stipulations in the "Installation Guidelines" section on page 2-3 and in the "SFP Module Slots" section on page 1-3. See Appendix B, "Connector and Cable Specifications" for information about the LC on the SFP module.

Step 1 Remove the rubber plugs from the module port and fiber-optic cable, and store them for future use.

Step 2 Insert one end of the fiber-optic cable into the SFP module port (see Figure 2-11).

Figure 2-11 Installing an SFP Module



1	Fiber-optic SFP module

Step 3 Insert the other cable end into a fiber-optic receptacle on a target device.

Step 4 Observe the port status LED.

- The LED turns green when the blade switch and the target device have an established link.
- The LED turns amber while the STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.
- If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 3, “Troubleshooting,” for solutions to cabling problems.

Step 5 If necessary, reconfigure and restart the blade switch or target device.

Where to Go Next

If the default configuration is satisfactory, the blade switch does not need further configuration. You can use any of these management options to change the default configuration:

- Using the Device Manager

  Access the device manager through a web browser from anywhere in your network. Follow these steps:

  a. Launch a web browser on your PC or workstation.

  b. Enter the blade switch IP address in the web browser, and press **Enter**. The device manager page appears.

  c. Use the device manager to perform basic blade switch configuration and monitoring. See the device manager online help for more information.

- Using the Management Blade Web Interface

  You can monitor and manage the blade switches through the BX600 system web interface. Follow these steps:

  a. Launch a web browser on your PC or workstation.

  b. Enter the BX600 system IP address in the web browser, and press **Enter**. The web interface appears.

  c. Click **Switch Blade 1**, **Switch Blade 2**, and so on to see the information for a specific blade switch.

  See the *PRIMERGY BX Blade Server Systems RemoteView Management Blade User Interface Description* for more information.

- Using the Command-Line Interface

  The blade switch CLI) is based on Cisco IOS software and enhanced to support desktop-switching features. You can fully configure and monitor the blade switch from the CLI. You can access the CLI either by connecting your management station directly to the blade switch console port or by using Telnet from a remote management station. Refer to the blade switch command reference on Cisco.com for more information.

- Using SNMP

  You can use SNMP management applications such as CiscoWorks Small Network Management Solution (SNMS) to configure and manage the blade switch. You also can manage it from an SNMP-compatible workstation that is running platforms such as HP OpenView or SunNet Manager.

Troubleshooting

The LEDs on the front panel provide troubleshooting information about the blade switch. They show failures in the power-on self-test (POST), port-connectivity problems, and overall blade switch performance. For a full description of the blade switch LEDs, see the "LEDs" section on page 1-4.

You can also get statistics from the browser interface, from the command-line interface (CLI), or from a Simple Network Management Protocol (SNMP) workstation. Refer to the blade switch software configuration guide, the blade switch command reference guide on Cisco.com, or the documentation that came with your SNMP application for details.

This chapter describes these topics for troubleshooting problems:

- Understanding POST Results, page 3-1
- Diagnosing Problems, page 3-1
- Locating the Blade Switch Serial Number, page 3-5

Understanding POST Results

As the blade switch powers on, it begins the POST, a series of tests that runs automatically to ensure that the blade switch functions properly. When the POST completes successfully, the System Status/ID LED is off, and the Console LED is solid green or amber. If the blade switch fails POST because of a misconfiguration or error, the System Status/ID LED blinks green, and the Console LED is off.

Note POST failures are usually fatal. Call Cisco Systems if your blade switch does not pass POST.

Diagnosing Problems

The LEDs on the front panel provide troubleshooting information about the blade switch. They show POST failures, port-connectivity problems, and overall blade switch performance. For a full description of the blade switch LEDs, see the "LEDs" section on page 1-4.

You can also get statistics from the browser interface, from the CLI, or from an SNMP workstation. Refer to the software configuration guide, the blade switch command reference guide on Cisco.com, or the documentation that came with your SNMP application for details.

You can access the Technical Support Website (http://www.cisco.com/tac) for a list of known hardware problems and extensive troubleshooting documentation, including:

- Field notices
- Security advisories
- Troubleshooting resources
- Factory defaults
- Password recovery
- Recovery from corrupted or missing software
- Switch port problems
- Network interface cards
- Troubleshooting tools

Common blade switch problems fall into these categories:

- Poor performance
- No connectivity
- Corrupted software

Table 3-1 describes how to detect and resolve these problems.

Table 3-1 Common Problems and Their Solutions

Symptom	Possible Cause	Resolution
Poor performance or excessive errors	Duplex autonegotiation mismatch.	Refer to the blade switch software configuration guide for information on identifying autonegotiation mismatches.
	Cabling distance exceeded	
	• Port statistics show excessive frame check sequence (FCS), late-collision, or alignment errors.	• Refer to the blade switch software configuration guide for information on displaying port statistics.
	• For 10/100/1000BASE-T connections:	
	– The distance between the port and the attached device exceeds 328 feet (100 meters).	• Reduce the cable length to within the recommended distances.
	– If the blade switch is attached to a repeater, the total distance between the two end stations exceeds the cabling guidelines.	• Refer to your repeater documentation for cabling guidelines.
	• For SFP port connections: – The distance between the SFP module port and the attached device exceeds the SFP module cabling guidelines.	• Refer to your SFP documentation for cabling guidelines.
	Bad adapter in attached device	
	• Excessive errors found in port statistics.	• Run adapter card diagnostic utility.
	• STP checking for possible loops.	• Wait 30 seconds for the port LED to turn green.

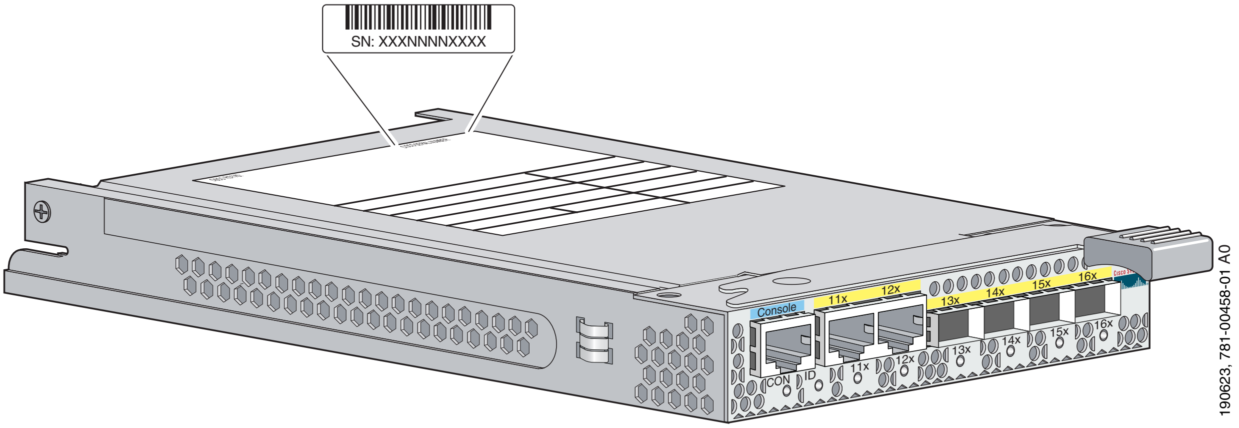
Table 3-1 Common Problems and Their Solutions (continued)

Symptom	Possible Cause	Resolution
No connectivity	**Incorrect or bad cable** These are results of no link at both ends:	
	- A crossover cable was used when a straight-through was required, or vice-versa.	- For the correct pinouts and the proper application of crossover or straight-through cables, see the "Two Twisted-Pair Cable Pinouts" section on page B-3.
	- The cable is wired incorrectly.	- Replace with a tested good cable.
	- A crossover or straight-through cable is wired incorrectly.	- For 1000BASE-T connections, be sure to use a twisted four-pair, Category 5 cable.
	- STP checking for possible loops.	- Wait 30 seconds for the port LED to turn green.
Unreadable characters on the management console	Incorrect baud rate.	Reset the emulation software to 9600 baud.
Amber system LED	Fatal POST error detected.	Contact Cisco Systems.
The blade switch port is placed in error-disabled state after SFP module is inserted	Bad or non-Cisco-approved SFP module.	Remove the SFP module from the blade switch, and replace it with a Cisco-approved module. Use the **errdisable recovery cause gbic-invalid** global configuration command to verify the port status, and enter a time interval to recover from the error-disabled state. Refer to the blade switch command reference guide for information on the **errdisable recovery** command.
Switch does not recognize the SFP module	The SFP module might be installed upside down. The SFP module does not snap into the slot.	Verify that the SFP module is not installed upside down. Remove the SFP module. Inspect for physical damage to the connector, the module, and the module slot. Replace the SFP module with a known good SFP module.

Locating the Blade Switch Serial Number

If you contact Cisco Technical Assistance, you need to know the serial number of your switch. See Figure 3-1 to locate the serial number on your switch. You can also use the **show version** command to get the serial number.

Figure 3-1 Serial Number Location on the Cisco Catalyst Blade Switch 3040 for FSC



Technical Specifications

This appendix lists the blade switch technical specifications in Table A-1.

Table A-1 Technical Specifications for the Cisco Catalyst Blade Switch 3040 for FSC

Environmental Ranges	
Operating temperature	32 to 113°F (0 to 45°C)
Storage temperature	–4 to 158°F (–20 to 70°C)
Relative humidity	10 to 90% (noncondensing)
Storage relative humidity	10 to 95% (noncondensing)
Operating altitude	10,000 feet (3048 meters)
Storage altitude	15,000 feet (4572 meters)
Physical Dimensions	
Weight	2 lbs (0.90 kg)
Dimensions (H x D x W)	1.35 x 5.12 x 10.93 in. (3.4 x 13 x 27.8 cm)

See the *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3040 for FSC* guide for information about safety compliance and electromagnetic compatibility.

APPENDIX B

Connector and Cable Specifications

This appendix describes the blade switch ports and the cables and adapters that you use to connect the blade switch to other devices.

Connector Specifications

These sections describe the connectors used with the blade switch.

10/100/1000 Ports

The 10/100/1000 Ethernet ports on the blade switch use standard RJ-45 connectors. Figure B-1 shows the pinout.

Note You can use the **mdix auto** interface configuration command in the CLI to enable the automatic medium-dependent interface crossover (auto-MDIX) feature. When the auto-MDIX feature is enabled, the blade switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a copper 10/100/1000 or 1000BASE-T SFP module port on the blade switch, regardless of the type of device on the other end of the connection.

For configuration information for this feature, refer to the blade switch software configuration guide or the command reference.

Connecting to 10BASE-T- and 100BASE-TX-Compatible Devices

When you connect the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as servers, workstations, and routers, you can use a two or four twisted-pair, straight-through cable wired for 10BASE-T and 100BASE-TX. Figure B-3 shows the two twisted-pair, straight-through cable schematics. Figure B-5 shows the four twisted-pair, straight-through cable schematics.

When you connect the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as switches or repeaters, you can use a two or four twisted-pair, crossover cable. Figure B-4 shows the two twisted-pair, crossover cable schematics. Figure B-6 shows the four twisted-pair, crossover cable schematics.

You can use Category 3, 4, or 5 cabling when connecting to 10BASE-T-compatible devices. You must use Category 5 cabling when you connect to 100BASE-TX-compatible devices.

Connecting to 1000BASE-T Devices

When you connect the ports to 1000BASE-T devices, such as servers, workstations, and routers, you must use a four twisted-pair, Category 5, straight-through cable wired for 10BASE-T, 100BASE-TX, and 1000BASE-T. Figure B-5 shows the straight-through cable schematics.

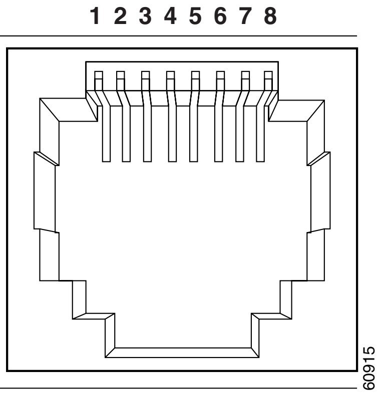
When you connect the ports to other devices, such as switches or repeaters, you must use a four twisted-pair, Category 5, crossover cable. Figure B-6 shows the crossover cable schematics.

Note Be sure to use a four twisted-pair, Category 5 cable when connecting to a 1000BASE-T-compatible device.

Note Use a straight-through cable to connect two ports only when one port is designated with an X. Use a crossover cable to connect two ports when both ports are designated with an X or when both ports do not have an **X**.

Figure B-1 10/100/1000 Port Pinouts

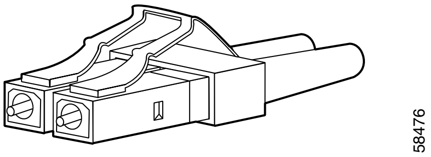
Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



SFP Module Ports

The blade switch uses SFP modules for fiber-optic ports. Refer to the blade switch release notes for a list of supported SFP modules.

Figure B-2 Fiber-Optic SFP Module LC Connector



Console Port

The console port uses an 8-pin RJ-45 connector, which is described in Table B-1 and Table B-2. The supplied RJ-45-to-DB-9 adapter cable is used to connect the console port of the blade switch to a console PC. You need to provide a RJ-45-to-DB-25 female DTE adapter if you want to connect the blade switch console port to a terminal. You can order a kit (part number ACS-DSBUASYN=) containing that adapter from Cisco. For console port and adapter pinout information, see Table B-1 and Table B-2.

Cable and Adapter Specifications

These sections describe the cables and adapters used with the blade switch.

Two Twisted-Pair Cable Pinouts

Figure B-3 and Figure B-4 show the schematics of two twisted-pair cables for connecting to 10BASE-T- and 100BASE-TX-compatible devices.

Figure B-3 Two Twisted-Pair Straight-Through Cable Schematic

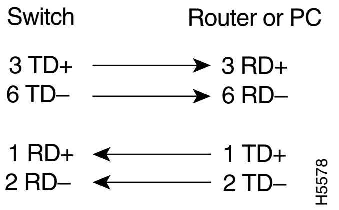
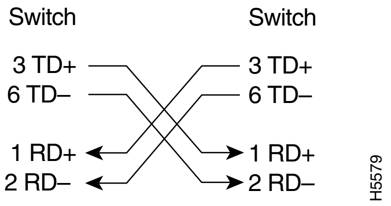


Figure B-4 Two Twisted-Pair Crossover Cable Schematic



Four Twisted-Pair Cable Pinouts for 1000BASE-T Ports

Figure B-5 and Figure B-6 show the schematics of four twisted-pair cables for 10/100/1000 ports on the blade switch.

Figure B-5 Four Twisted-Pair Straight-Through Cable Schematic for 10/100/1000 Ports

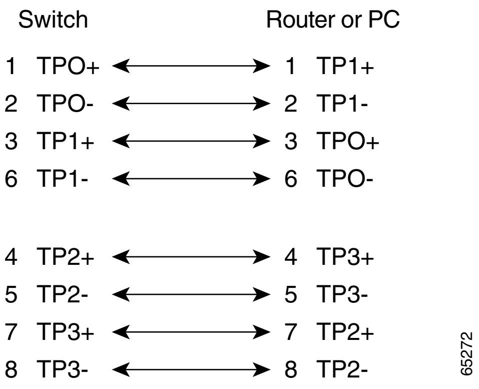
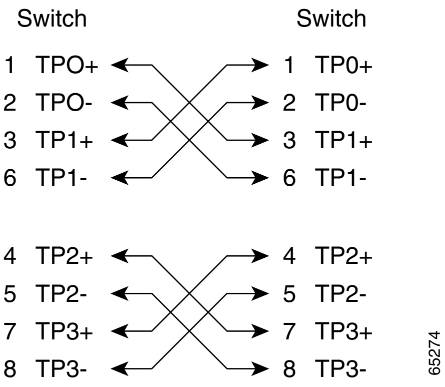


Figure B-6 Four Twisted-Pair Crossover Cable Schematics for 10/100/1000 Ports



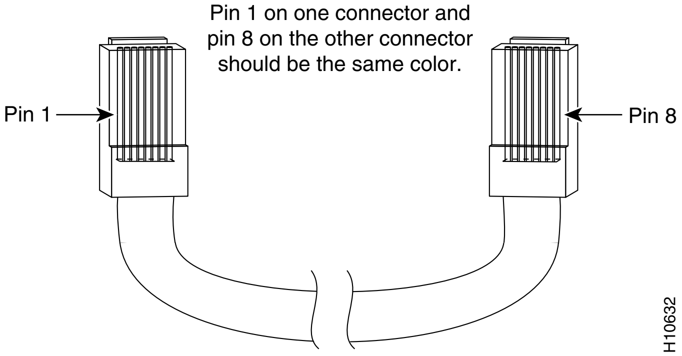
Crossover Cable and Adapter Pinouts

This section describes how to identify a crossover cable and also describes the adapter pinouts.

Identifying a Crossover Cable

To identify a crossover cable, compare the two modular ends of the cable. Hold the cable ends side-by-side, with the tab at the back. The wire connected to the pin on the outside of the left plug should be the same color as the wire connected to the pin on the outside of the right plug. (See Figure B-7.)

Figure B-7 Identifying a Crossover Cable


Pin 1 on one connector and pin 8 on the other connector should be the same color.
Pin 1
Pin 8
H10632

Adapter Pinouts

Table B-1 lists the pinouts for the console port, the RJ-45-to-DB-9 adapter cable, and the console device.

Table B-1 Console Port Signaling Using a DB-9 Adapter

Switch Console Port (DTE)	RJ-45-to-DB-9 Terminal Adapter	Console Device
Signal	**DB-9 Pin**	**Signal**
RTS	8	CTS
DTR	6	DSR
TxD	2	RxD
GND	5	GND
GND	5	GND
RxD	3	TxD
DSR	4	DTR
CTS	7	RTS

Table B-2 lists the pinouts for the console port, RJ-45-to-DB-25 female DTE adapter, and the console device.

Note The RJ-45-to-DB-25 female DTE adapter is not supplied with the blade switch. You can order a kit (part number ACS-DSBUASYN=) containing this adapter from Cisco.

Table B-2 Console Port Signaling Using a DB-25 Adapter

Switch Console Port (DTE)	RJ-45-to-DB-25 Terminal Adapter	Console Device
Signal	**DB-25 Pin**	**Signal**
RTS	5	CTS
DTR	6	DSR
TxD	3	RxD
GND	7	GND
GND	7	GND
RxD	2	TxD
DSR	20	DTR
CTS	4	RTS

APPENDIX C

Configuring the Switch with the CLI-Based Setup Program

This chapter provides a quick installation and setup procedure for the blade switch by using the command-line interface (CLI).

Note For detailed installation procedures, see Chapter 2, "Blade Switch Installation." For product overview information, see Chapter 1, "Product Overview."

These are the major steps for a quick installation when using the CLI:

1. Accessing the CLI Through the Console Port, page C-1
2. Taking Out What You Need, page C-1
3. Connecting to the Console Port, page C-2
4. Completing the Initial Configuration, page C-4

Accessing the CLI Through the Console Port

You can access the CLI on a configured or unconfigured blade switch by connecting the console port of the blade switch to the serial port on your PC or workstation and accessing the blade switch through a Telnet session.

Taking Out What You Need

These items ship with your blade switch:

- Console cable
- *Cisco Catalyst Blade Switch 3040 for FSC Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3040 for FSC*
- Registration card

Follow these steps:

1. Unpack and remove the blade switch and the accessory kit from the shipping box.
2. Return the packing material to the shipping container, and save it for future use.

Note If the blade switches are ordered with the blade server, the blade switches are already installed, and no unpacking is required. The unpacking procedure applies only if a blade switch is ordered separately.

Note You need to provide the Category 5 straight-through cables to connect the blade switch ports to other Ethernet devices.

Connecting to the Console Port

Obtain and make note of this information from your network administrator before you begin the blade switch installation:

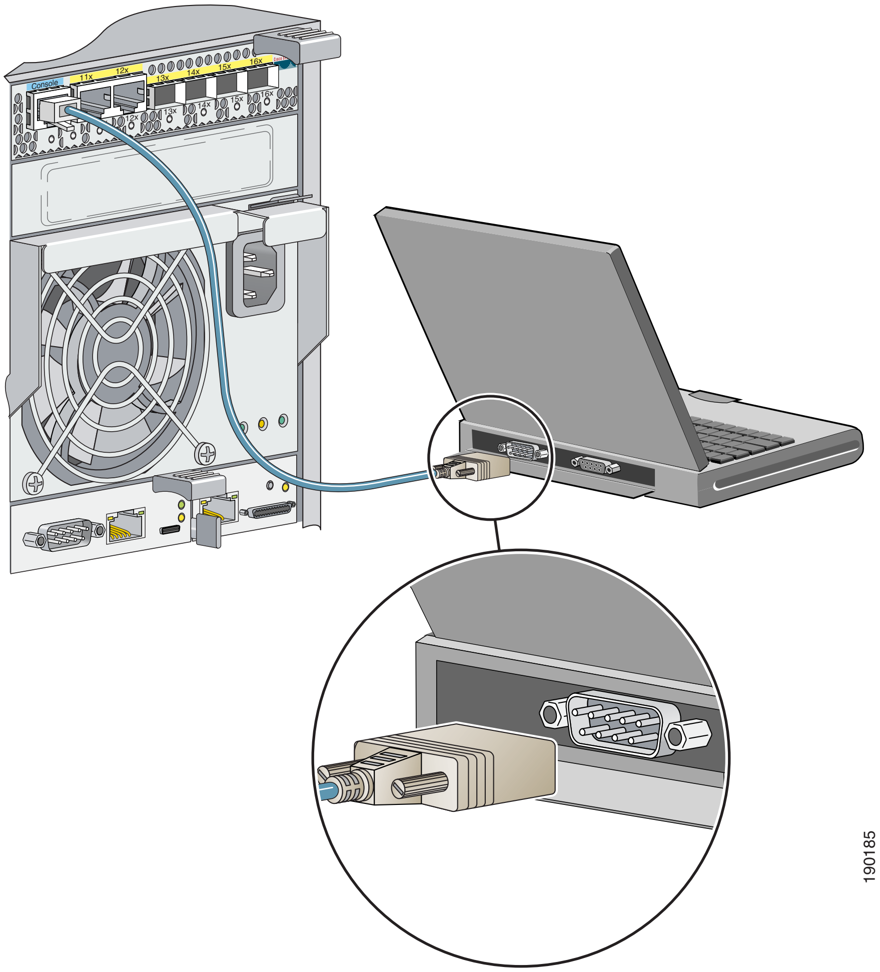
- Switch IP address
- Subnet mask (IP netmask)
- Default gateway (router)
- Enable secret password (encrypted)
- Enable password (not encrypted)
- Telnet password
- SNMP community strings (optional)

Step 1 Connect one end of the console cable to the blade switch console port. Connect the other end of the cable to the serial port of the computer that is running the terminal emulation application. (See Figure C-1.)

You can use the **mdix auto** interface configuration command in the CLI to enable the automatic medium-dependent interface crossover (auto-MDIX) feature. When the auto-MDIX feature is enabled, the blade switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a copper 10/100/1000 or 1000BASE-T SFP module port on the blade switch, regardless of the type of device on the other end of the connection.

For configuration information for this feature, refer to the blade switch software configuration guide or the blade switch command reference.

Figure C-1 Connecting through the Blade Switch Console Port



Step 2 Start the terminal emulation session so that you can see the output display from the power-on self-test (POST). The terminal-emulation software—a PC application such as Hyperterminal or ProcommPlus—makes communication between the blade switch and your PC or terminal possible.

Configure the baud rate and character format of the PC or terminal to match these console port default characteristics:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- None (flow control)

Step 3 Wait for the blade switch to complete the POST. It might take several minutes for the blade switch to complete POST.

Step 4 Verify that POST has completed by confirming that the system and status LEDs remain green.

If the blade switch fails POST, the system LED turns amber. POST errors are usually fatal. Call Cisco Systems immediately if your blade switch fails POST.

Step 5 Wait for the switch to complete flash initialization. When you see the prompt, `Press Return to Get Started!`, press **Return** or **Enter**.

Step 6 Make sure that the system and status LEDs are green. The blade switch is now operating properly.

Step 7 See the "Completing the Initial Configuration" section on page C-4 for instructions on setting up and initially configuring the blade switch.

Completing the Initial Configuration

Follow these steps to complete the setup program and to create an initial configuration for the blade switch.

Note For information about automatically configuring the blade switch, see the "Assigning the Switch IP Address and Default Gateway" chapter in the blade switch configuration guide.

Step 1 After you have pressed **Enter** or **Return** after the prompt to start the initial configuration setup program, enter **yes** at these prompts:

```
Would you like to terminate autoinstall? [yes]: yes
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
```

Step 2 Enter a hostname for the blade switch after the prompt, and press **Return**.

The hostname is limited to 20 characters. Do not use *-n*, where n is a number, as the last character in a hostname for any blade switch.

Step 3 Enter an enable secret password, and press **Return**.

The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows spaces, but ignores leading spaces. The secret password is encrypted, and the enable password is in plain text.

Step 4 Enter an enable password, and press **Return**.

Step 5 Enter a virtual terminal (Telnet) password, and press **Return**.

The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

Step 6 (Optional) Configure Simple Network Management Protocol (SNMP) by responding to the prompts.

1. To configure SNMP later, press **Return** (which applies the default of no). If you accept the default, you can configure SNMP later through the CLI.

```
Configure SNMP Network Management? [no]:
```

2. To configure SNMP now, enter **yes**.

```
Configure SNMP Network Management? [no]: yes
Community string [public]: public
```

Step 7 Enter the interface name (physical interface or VLAN name) of the interface that connects to the management network, and press **Return**.

Enter **vlan1** for the interface name at this prompt.

Step 8 To configure the interface, enter **Yes** after the prompt, and then enter the blade switch IP address and subnet mask. Press **Return**.

The IP address and subnet mask shown here are examples:

```
Configuring interface Vlan1:
Configure IP on this interface? [yes]:
IP address for this interface [10.0.0.1]:
Subnet mask for this interface [255.255.255.0] : 255.255.255.0
Class A network is 10.0.0.1, 21 subnet bits; mask is /21
```

Step 9 Enter **no** when the prompt asks you if you would like to enable the blade switch as a cluster command switch. This blade switch is a standalone switch.

```
Would you like to enable as a cluster command switch? [yes/no]: no
```

Note The Cisco Catalyst Blade Switch 3040 for FSC does not support clustering.

You have now completed the initial configuration of the blade switch, which displays its initial configuration. An example of the output is shown here:

```
The following configuration command script was created:
hostname switch1
enable secret 5 $1$cagJ$e4LP91PNazfdADoNAZm6y0
enable password enable_password
line vty 0 15
password terminal-password
snmp-server community public
!
!
interface Vlan1
no shutdown
ip address 10.0.0.1 255.255.255.0
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2

. . . (output truncated)



interface GigabitEthernet0/16
!
end
```

Step 10 These choices appear:

```
[0] Go to the IOS command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

If you want to save the configuration and use it the next time the switch reboots, save it
in NVRAM by selecting option 2.

Enter your selection [2]:2
```

Make your selection, and press **Return**.

Step 11 Disconnect the blade server serial port or the blade switch console port from the PC. See the "Management Options" section on page 1-5 for information about managing the blade switch.

INDEX